



# Security Breach Response A Five Step Approach

*Presented to ACCA – SoCal*

*by Pillsbury Winthrop Shaw Pittman LLP*

*Wayne Matus*

*Catherine Meyer*

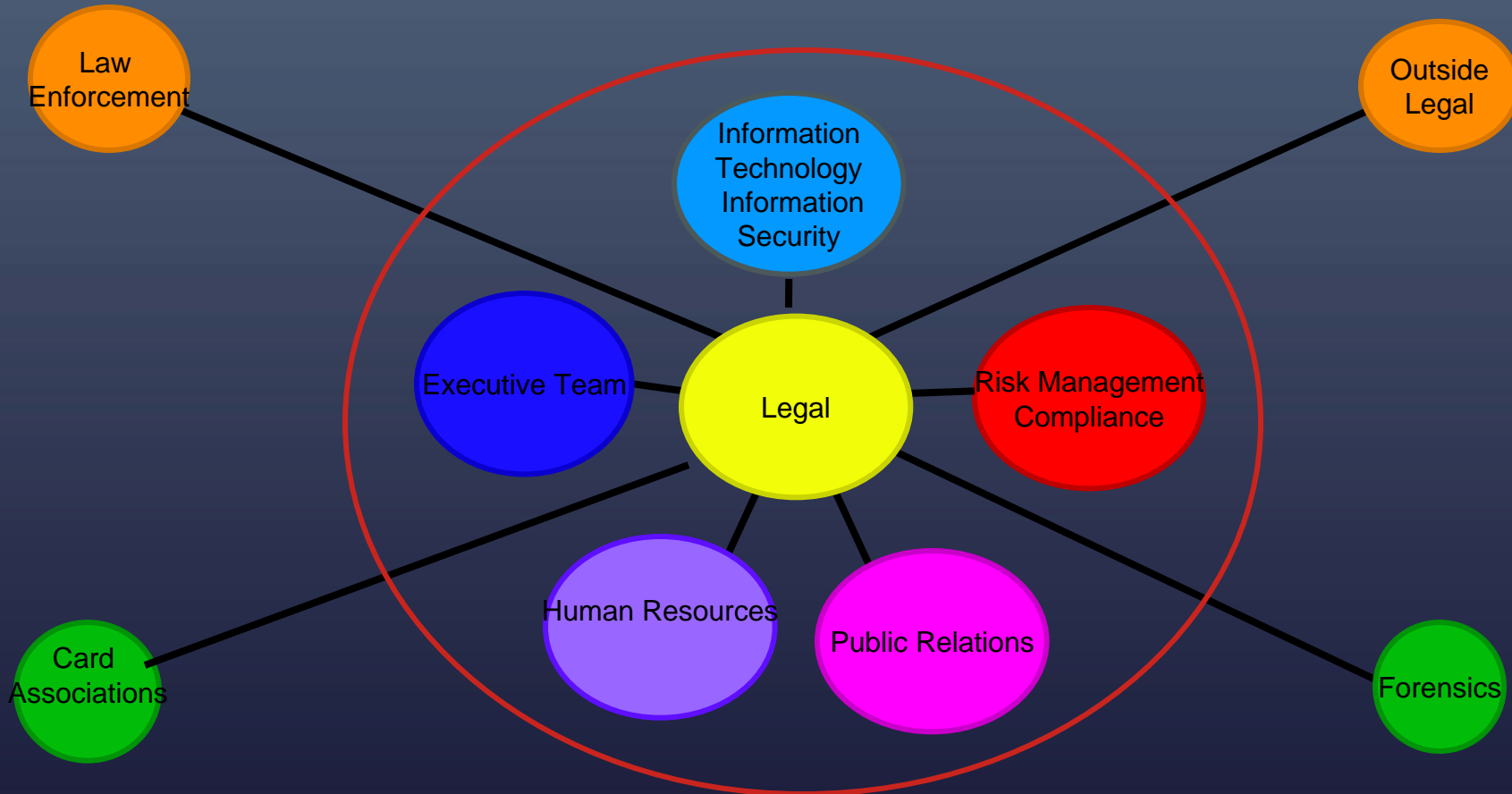
*Deborah Thoren-Peden*

*September 17, 2008*

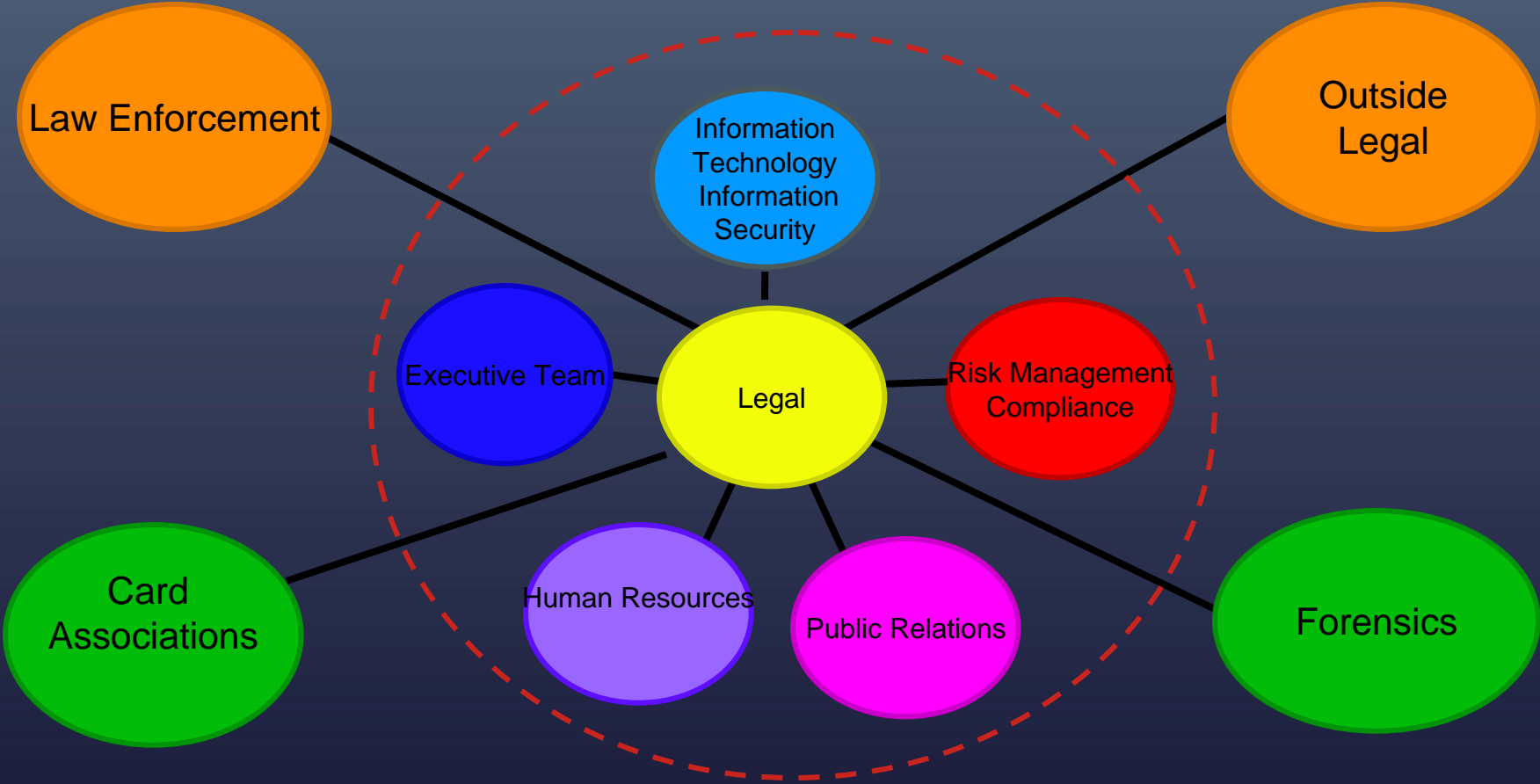
# Five Steps To Security Breach Response

- 1. Incidence Response Team
- 2. Be Prepared – Anticipating problems
- 3. Discovery and Investigation
- 4. Consumer Notification
- 5. Post-mortem: Learning from mistakes, applying best practices

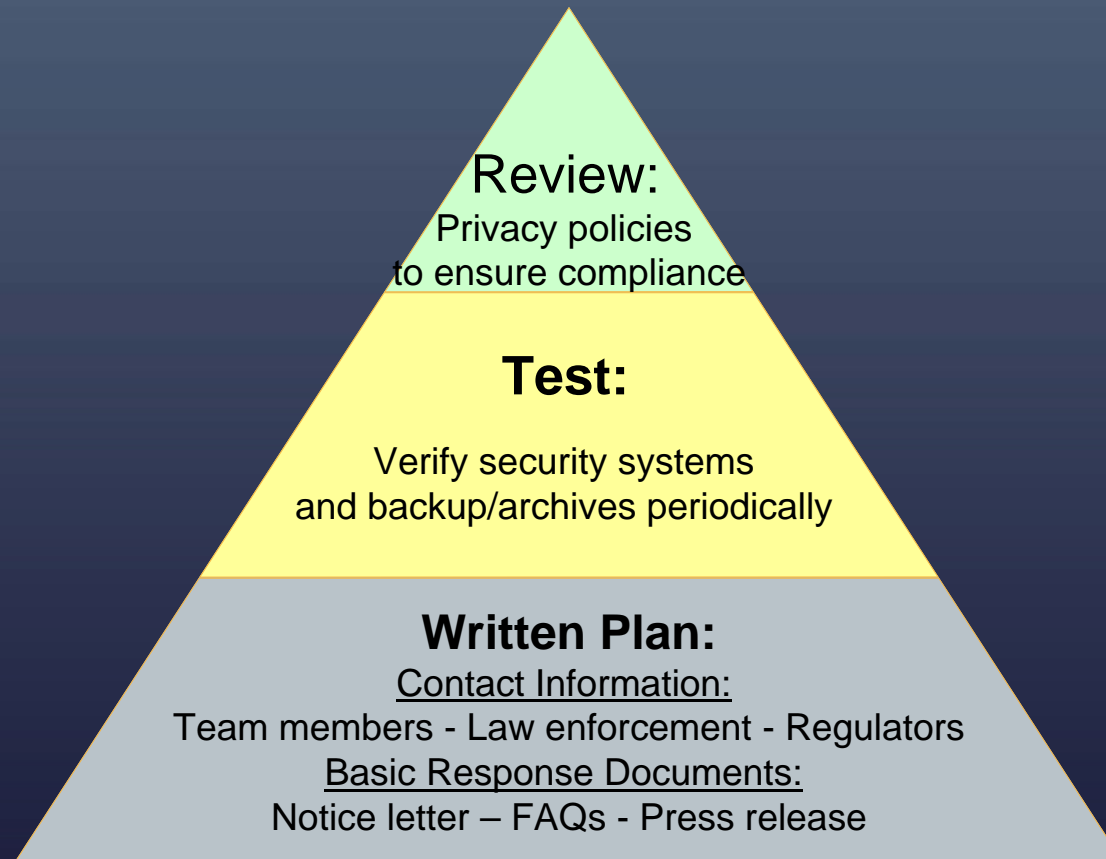
# Incidence Response Team Internal Members



# Incidence Response Team External Members



# Be Prepared: Your Best Defense



# Discovery and Investigation: Keep your fingers off the crime scene

- Notify Team
- Designate point person for:
  - Technical investigation
  - External communications
  - Regulators
  - Law enforcement
  - Restoration of system
- Engage Forensic consultant to preserve evidence of event
- Communications issues

# Investigation

- TIME IS CRITICAL
- FIRST: Shut down system
- SECOND: Preserve system image and logs
  - Inexperienced review of system can overwrite tracks of invader
- Analyze each system
- Determine nature and scope of compromise
- Restrict access until investigation is complete
- Document sequence of intrusion/event and all remedial steps taken
  - Incident documentation retention required in a number of states – up to 5 years

# Consumer Notification

## Seven Key Questions:

1. What information was involved?
2. Was data improperly accessed, acquired or disclosed?
3. Likelihood of misuse?
4. Was data protected
  - Passwords, Encryption, Redaction
5. Where do individuals reside?
6. Are credit cards involved?
7. Do we have contact information (mailing address) for all involved?

# Notice to Consumers: Legal Review

- 44 States plus Washington DC and Puerto Rico have varying statutes
  - Law of state of residence of individuals governs
  - Access vs. Acquired vs. Risk of Harm/Misuse
  - Computerized data vs. any format
  - Types of data triggering notice (some states also include medical records, passport numbers, biometrics, email or ISP accounts)
- Additional notices to agencies is sometimes required
  - May depend on number of affected state residents or total number notified.
  - Timing of notifications – special state forms
  - State agency involvement in decision not to give consumer notice
- Notice to Consumer Reporting Agencies sometimes required

# Notice to Consumers

- **Form of notice**
  - Written, email, substitute
  - State by state compliance required
- **Timing of sending notice**
  - Without unreasonable delay
  - Statutory deadlines (45 days in some states)
  - “Recommended” deadlines (10 business days in other states)
  - Immediate notification of agencies sometimes required (NJ State Police)
- **Central point of contact for consumer questions**
  - Website, call center, company phone bank
- **Credit monitoring assistance**
  - Not legally required
  - Customer relations issue
  - Varies with type and circumstance of breach

# Law enforcement and the Press

- Law Enforcement:
  - Notify as soon as practical
  - coordinate investigation with them if they so instruct
  - State consumer fraud units
  - Secret Service
- Press relations
  - be ready with a press release of contacted
  - strive for one report with no follow up
- Additional Exposure
  - FTC or state Attorneys General are taking note of breaches to determine potential deceptive practice actions

# Post-mortem:

## Review response effort and learn

- Test restored system
- HR Training or additional screening procedures
- Review and revise:
  - vendor contracts
  - policies
  - basic documentation
  - written response plan
- Learn from responses from
  - affected people
  - press coverage
- Evaluate overall response effort

# Contact us with Questions

## **Wayne Matus**

Partner, Pillsbury

212.858.1774 | fax 212.858.1500

wayne.matus@pillsburylaw.com

## **Catherine D. Meyer**

Counsel, Pillsbury

213.488.7362 | fax 213.226.4160

catherine.meyer@pillsburylaw.com

## **Deborah Thoren-Peden**

Partner, Pillsbury

213.488.7320 | fax 213.629.1033

deborah.thorenpaden@pillsburylaw.com